A survey of RFID readers anticollision protocols

Abdoul Aziz Mbacke[1,2], Nathalie Mitton[1], Hervé Rivano[1,2]
[1]*Inria*, [2]*Univ Lyon, INSA Lyon, CITI*
firstname.lastname@inria.fr

***Abstract*—While RFID technology is gaining increased attention from industrial community deploying different RFID-based applications, it still suffers from reading collisions. As such, many proposals were made by the scientific community to try and alleviate that issue using different techniques either centralized or distributed, monochannel or multichannels, TDMA or CSMA. However, the wide range of solutions and their diversity make it hard to have a clear and fair overview of the different works. This paper surveys the most relevant and recent known state-of-the-art anti-collision for RFID protocols. It provides a classification and performance evaluation taking into consideration different criteria as well as a guide to choose the best protocol for given applications depending on their constraints or requirements but also in regard to their deployment environments.**

***Keywords*—RFID Radio Frequency Identification; reader anticollision problem; MAC layer; resource allocation; distributed systems; mobile systems**

I. INTRODUCTION

The democratization of RFID systems is turning it into a ubiquitous technology met in various everyday applications. Indeed, from the obvious limitations of traditional barcodes, RFID came to the rescue, offering wireless and non-line of sight identification of goods and people. These key factors have made it highly attractive for several applications ranging from retail to supply chain management, going through inventory management, security or infrastructure monitoring.

Another key factor of the large democratization of RFID is its simple architecture that relies on just two main components:

- **tags**: they are electronic labels storing a unique identifier called electronic product code (EPC). This data is accessed wirelessly by their counterparts upon request. Tags usually encompass three main components: on-board micro-controller, memory storing the data, and transceiver. Most of the tags are considered to be unintelligent entities, which limits them to be powered upon request and answer using the same energy to share their data. Their small size and low cost make them a great option for tracking a whole range of products. Some tags also carry a battery and are referred to as active tags, allowing them to initiate communication and thus transmit without waiting for a request. However, these latter active tags are out of the scope of this paper which in the remaining will only address passive tags.

- **readers**: they are the counterparts that access the information stored in tags. As their name implies they are in charge of "reading" the data enclosed in tags. During reading procedure, the reader sends a request towards tags. The electromagnetic signal generated by the reader is then used by the tag to power its components, to access the stored information and send it back to the reader. This process is known as "backscattering" [1].

Regarding the operating frequency of radio signals, we identify three operating bands being either Low Frequency (LF), High Frequency (HF) or Ultra High Frequency (UHF). LF tags (125kHz - 135kHz) usually have a shorter range of tenths of centimeters at most but perform better in hostile environments such as metal or liquids; HF tags (13.56MHz) have a longer transmission range, up to 1 meter, they are an improvement over LF tags with a smaller form factor; UHF tags (860MHz - 960MHz) have a transmission range of up to several meters and are even smaller in size.

Nowadays, RFID systems can be met on a regular basis throughout the city. Most retail stores rely on a set of RFID tags deployed on their goods. This allows for a tracking of the available stock but also as a security mechanism preventing shoplifting, thanks to RFID readers deployed at exits, identifying goods and signaling any abnormality. In supply chains nowadays, RFID tags are also used to track position and status of goods. As an example, tags can be attached to crates stored in a warehouse with readers used to track entries and exits. They also allow finding a unique product in the warehouse thanks to mobile readers roaming through the aisles.

In the following of this paper, we will mainly target passive tags which are more compliant than active tags, which necessitate a battery, for IoT applications requirements to improve energy efficiency. UHF RFID systems operating in the frequency band of $865-868$MHz or $902-928$MHz, according respectively to ETSI [2] or FCC regulations are considered a better choice than LF or HF systems, with lower ranges, for IoT applications thanks to the longer interrogation range. Multiple works have been conducted towards ambient energy harvesting and in particular [3] discusses harvesting energy in UHF RFID. Previously in [4], authors present how sensors could be attached to passive RFID tags in order to get both the original identification but also battery-free environmental sensing. A comparative study of sensing using the different RFID bands is done in [5]. Authors also present the case of wireless temperature and pressure sensors using passive battery-free RFID sensors for industrial applications.

Today, sensors attached to passive tags can be found enabling a whole new range of sensing applications. Indeed, several applications can be found with RFID being evaluated in challenging environments such as embedded in concrete [6], disposed in water [7], buried underground [8] or attached to metallic materials [9]. As such, urban infrastructures such as

Aloha based	Tree based	Hybrids
Pure Aloha	Tree splitting	Tree-slotted Aloha
Slotted Aloha	Query tree	Hybrid Query Tree (HQT)
Frame-slotted Aloha	Binary search	HQT variants
-	Bitwise arbitration	Hash tree

TABLE I: Tag anti-collision protocols

buildings, bridges, roads, etc. can all be monitored thanks to passive RFID sensing tags with readers either fixed at specific endpoints or attached to roaming vehicles like the public transportation lines. Their low cost and ease of deployment also make them a consistent challenger to traditional Wireless Sensor Network (WSN) solutions. However, deploying large numbers of readers in an area to monitor and retrieve information stored in tags comes at a cost. Indeed, the backscattering that made RFID so attractive compared to traditional barcodes or WSN solutions, is also one of the main drawbacks of this technology. Indeed, as with any other wireless communication, RFID suffers from collisions. These latter can be observed on two different levels when looking at RFID systems:
- **Tag collisions**: they happen when a reader tries to identify multiple tags at the same time. Without a proper mechanism, all interrogated tags respond simultaneously generating collisions at the reader level. This can result in unread tags, increased delay, not to mention the energy waste.
- **Reader collisions**: in order to ensure proper coverage of the deployed tags to avoid blind spots and misreadings, several readers are deployed in close proximity. Applications, like the warehouse described above, can also require the installation of multiple readers around gates to track stock entries and exits. As such, reader collisions are observed, they are the result of multiple readers attempting to access the same tags simultaneously. Without an anti-collision scheme, multiple requests from different readers arriving at the tags cannot be dissociated or recognized, as such they are considered as radio noise and discarded. Similar to tag collisions, these also result in unread tags, increased delay and energy waste to successfully cover all tags. This issue is still the subject of multiple proposals all made to alleviate the collisions while improving either the throughput, efficiency, fairness, etc of the system as we will see in the remaining of the paper.

In this paper, we focus on reader-to-reader collisions, reviewing the main state-of-the-art proposals made to alleviate this issue. Several proposals have surfaced to resolve reader-to-tag and tag-to-tag collisions issues and can be classified as seen in Table I. [10] gives an in-depth review of these different reader-to-tag anti-collision protocols. The reviewed reader-to-reader anti-collision algorithms are classified based on different criteria regarding if they are:
- **centralized** or **distributed**: all readers are managed by a central server that serves as a coordinator or each reader runs a local algorithm based on local information.
- **time division** or **carrier-sense based**: readers access tag at different times following a pre-established Time Division Multiple Access technique (TDMA) or readers listen the medium to check for its state beforehand which is called Carrier Sense Multiple Access (CSMA).
In the following of this manuscript, we will address reader-to-reader collisions as reader collisions. This paper surveys the different schemes according to their operating principle, performance and scalability.

The only RFID reader anti-collision surveys, to the best of our knowledge, were done in [11] and [12], no other recent work proposing an overview of RFID anti-collision protocol are available. Authors at the time presented different collision management techniques. However, these reviews are now outdated with the current state-of-the-art approaches. Indeed, in our work, we propose to cover most of the known as well as some recent state-of-the-art protocols and compare them according to different criteria. This paper also proposes to guide the choice of an RFID reader anti-collision scheme based on the characteristics of the deployment as well as the application requirements. Indeed, depending on the application specifications, different RFID reader anti-collision schemes can be used to provide reliable and sustainable performances as it will be discussed in the following.

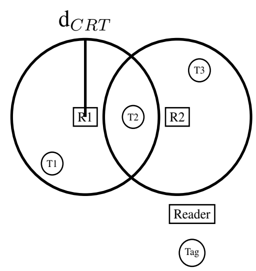
The main contributions of this paper are a state-of-the-art survey, as well as a classification of protocols according to their performance in regards to application requirements. It provides the following insights: in order to have the best performance in a dense and static deployment of readers with no regards to delay like an environmental sensing application (lake/river water levels, pollution monitoring, etc.) HiQ [13] or ACoRAS [14] are the most efficient solutions; for low density deployments with low to medium mobility and not collision sensitive applications (factories, manufacture lines, etc.) Pulse [15] or LBT [16]; for high mobility and density with low delay but not collision sensitive applications (smart cities, preventing forest fires, warehouse goods tracking, etc.) CORA [17] if the application is collision sensitive but not delay sensitive (harbor dock loading and unloading, etc.) GD-MRSOA-AIS [18] is the best trade-off.

The remainder of this paper is organized as follows: Section II reestablishes and details the collision issues and protocol design requirements before explaining RFID protocols categorization in Section III. Section IV & Section V respectively details TDMA and CSMA proposals distinguishing centralized from distributed algorithms. In Section VI, we further the discussion regarding the different proposals with a comparative study. Finally, Section VII draws conclusions over the present work.

II. CHALLENGES

A. *Dense environments*

The advent of smart cities and the need to improve productivity, traceablity, security and agility of casual setups induced a larger deployment of readers to ensure coverage over the deployment area. Raising the cardinality of deployed readers over a given area is referred to as "densification" in the following. While dense deployments are expected to enhance coverage and delay, they mainly result in generating collisions. As stated earlier, these collisions happen at different levels but in this paper, we will only focus on reading collisions. These latter occur when multiple readers attempt to read a given tag simultaneously. Since tags are passive entities, with no computation or frequency dissociation capabilities, they are unable to differentiate the different requests coming from the different readers, and will just identify the multiple requests as radio noise, which results in an unread tag. Over on Figure 1a, an example is shown where both readers R1 and R2 attempt to identify tags in their vicinity. While tags T1 and T3 are successfully read by readers R1 and R2 respectively, T2 which is within the colliding area of the readers fails to be read. In order to avoid such an issue, R1 and R2 should either operate at different times or with a distance of at least $d = 2 \times d_{CRT}$ with d_{CRT} being the reading range. Another solution would be to have readers operate at different frequencies [2]. However in a very dense network, the distribution of available frequencies can be quite laborious, taking into account the adjacent channel interference that can occur (see Section III-D), and the number of channels not sufficient. Thus having an efficient dynamic RFID reader anti-collision algorithm becomes crucial to improve tag identification.



(a) Reader collision

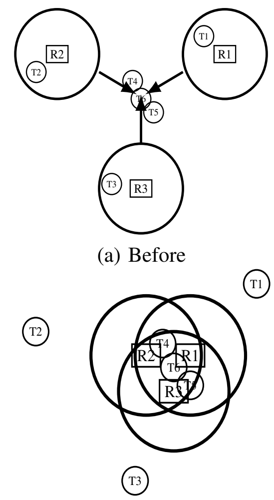
Fig. 1: RFID collisions

B. Mobility

In light of the applications described in Section I, we understand the need to have mobile readers alongside static ones. Indeed, in order to monitor a whole warehouse with tags attached to all products, relying solely on static deployed readers is highly inefficient both in terms of needed devices and cost. Having mobile readers being able to roam the aisles and reach all corners of the warehouse improves the agility of the system. In the same scope, in the case of a smart city with tags attached to urban infrastructures, the system cannot depend on fix readers, using public transportation vehicles or public bikes could help reach all deployed tags. However, the use of mobile readers, as for the densification, results in a increase of collisions. Indeed, when the mobility is not controlled to manage collisions of multiple readers scouting the same area, it induces unread tags and possibly uncovered ones issues, which defeats the original purpose of having mobile readers.

In Figure 2, a configuration of three mobile readers R1, R2 and R3 can be seen with six tags being deployed. At first (Figure 2a), R1, R2 and R3 will respectively be able to identify tags T1, T2 and T3. In order to cover the rest of tags, readers will then proceed to move towards the center, following the arrows depicted. In Figure 2b, we observe that following their movement, R1, R2 and R3 will have their readings colliding over T4, T5 and T6 which will fail to be identified as explained in Section II-A. This means that without a proper scheduling mechanism, despite having three mobile readers, only 50% of the tags are read in this configuration.

The design of a performing reader anti-collision algorithm should take the potential mobility of devices into account in order to overcome these conflicts.



(a) Before

(b) After

Fig. 2: Mobility induced collision

III. Protocol categorization

A. Time Division Multiple Access vs Carrier Sense Multiple Access

RFID reader anti-collision protocols can broadly be classified in two categories based on their operating scheme. They either rely on a time distribution and/or reservation based algorithm or on medium sensing in order to check for channel idleness before interrogating tags. In the former case, algorithms are considered as TDMA-based. In this configuration, the running operation time is divided into units of time referred as *timeslots*. These timeslots are either assigned or chosen by readers, based on the algorithm, in order to access the medium and interrogate tags. This scheme ensures that only one reader is operating within its vicinity during its timeslot since neighbor readers have either chosen different timeslots or were disabled during the contention procedure. Such schemes allow for a better energy management since readers can *sleep* and remain idle until their timeslot comes up and go back to idle. However, the main challenge in this configuration is the synchronization between readers which can be done using a server or internal clocks.

On the other hand, readers can *listen* the activity on the medium to ensure it is idle before interrogating tags. In this case, they are considered as CSMA-based. Since the medium is shared among readers, they can sense the activity of their neighbors and depending on the medium being idle or not they will be able to interrogate tags. In case the medium is sensed as occupied, readers wait for a random or defined period of time before listening again to check for channel activity. However, the main challenge with this solution is that in case of a dense deployment of readers, the waiting time for a reader might be long before it gets the chance to access tags which impacts the system performance. This makes it unsuitable for applications that involve the use of mobile tags. For example, in the case of a tags attached to vehicles in a city to have a sense of traceability, long waiting times for readers with fast moving cars could mean that several cars would not be identified.

Although we divided proposals following these two operating schemes, it is important to note that some approaches also rely on a Frequency Division Multiple Access (FDMA) to avoid collisions. Indeed, thanks to the different frequencies introduced by ETSI EN 302.208 [2], readers can operate on different channels to prevent reading collisions. Nevertheless, depending only on these different channels to avoid collisions is not enough in view of the possible dense deployment of RFID readers and their proximity. Some proposals took into account the multichannel aspect (see Sections III-C, IV and V) but still built upon a TDMA or CSMA scheme to schedule operations.

B. Centralized vs Distributed

In order to ensure the necessary coordination between readers to avoid collisions, a form of communication should be established between readers themselves or with a superior entity charged with their synchronization. The choice regarding this form of communication defines not only the nature of the algorithm but also affects its performance:

- **centralized**: in this configuration, readers communicate with a top entity (central server) responsible for the scheduling of operations. The central server is able, after gathering all information from the readers topology, to compute the optimal reading scheme reducing collisions. However, in general, the use of a central server restricts the mobility of readers at the expense of a higher level of computation and latency. A communication link also has to be set between the readers and this superior entity as discussed in Section III-D. Added to that, having readers depending on a superior entity for any operation makes solutions less reactive. Solutions depending on the use of a central server are usually found in TDMA-based schemes.
- **distributed**: in this setup, readers directly communicate with each other and locally (in time and space), agree in a peer to peer manner on their operation schemes to reduce collisions. Readers are able to exchange with their peers in the extent of their communication range defining their vicinity, this allows solutions based on this paradigm to be scalable and support dynamic changes in topology like it would be the case with mobile readers. Every decision taken by a given reader is dictated by its knowledge of its vicinity at a given time. Distributed solutions are found both in TDMA and CSMA-based algorithms.

C. Monochannel vs Multichannel

In the early versions of RFID systems, all readers had to identify tags using a common single channel. This single frequency medium became a scarce resource with dense deployments where several readers are in proximity and resulted in increasing collisions as shown in Figure 1. To overcome this deficiency, multichannel was introduced in the update of the standard brought by [2]. Readers are now able to interrogate tags on 4 different channels [2], making tag readings less competitive and subject to collisions. Indeed, by efficiently assigning these channels to readers in the same vicinity, the number of collisions can be reduced up to 4 times, thus enhancing the efficiency of RFID systems. However, having more frequencies does not prevent RFID readers from colliding. Indeed tags under concurrent readers, even on different channels, still cannot be read and are subject to another form of interference (see Section III-D). As such, collisions still remain and have to be addressed.

D. Dedicated control channel

In Section III-B, we explained the need for readers to either communicate with a central server or directly with each other. The hypothesis of a dedicated control channel between readers in a distributed scheme can be found in literature, as well as in a centralized scheme, with the dedicated channel being set between readers and the central server. Some proposals in the literature even considered the idea of both a link between readers and a central server as well as links between readers themselves.

The range of this dedicated control channel, in the case of a wireless setup, has to be set accordingly to allow proper exchange between readers and define the proper contention area for each reader. Indeed, as presented in Figure 1, if readers are not aware of their neighbors in a radius of at least d_{CRT} they might unknowingly collide with other devices. As such a proper communication range d_{COM} between readers in a single channel environment should at least be $d_{COM} = 2 \times d_{CRT}$. However, in the case of a multichannel algorithm, this value is insufficient due to adjacent channel interference that arise. This concern was investigated in [19], and the authors determined that to avoid adjacent channel interference, a distance of at least $d_{AC} = 3.3 \times d_{CRT}$ should be observed.

IV. TDMA PROPOSALS

A. Distributed algorithms

We first review distributed TDMA proposals. Multiple ones can be found but they mainly are derivatives from DCS and require a dedicated communication channel between devices to exchange local information.

1) Distributed Color Selection (DCS): In DCS [20], readers periodically reserve timeslots (here called *colors*) by randomly choosing among the range of available colors. These timeslots are then used in order to communicate with tags. As such, if two or multiple neighboring readers chose the same colors, their signals collide and covered tags are missed. In case of a collision, involved readers select a new color from the available ones and send a *kick* message to neighbors to reserve the timeslot for the following interrogation round. All readers on the corresponding color have to switch to a different timeslot for the following round. The number of available colors to chose from is fixed and given at the beginning. Depending on the maximum number of colors available, the RFID system is highly affected. Indeed, if the max colors value is too low, a high number of readers end up choosing the same colors and collide, while if the value is too high, some timeslots are not occupied and both throughput and coverage delay are impacted.

2) Colorwave: Also known as Variable-maximum DCS [20], this algorithm addresses the main issue of DCS. As the name implies, it allows the number of maximum available colors to be modified throughout the life of the RFID system. In order to set the maximum color value according to the state of the network, 2 thresholds variables are introduced *UpSafe* & *DnSafe*. Each reader monitors its number of successful interrogations, depending on if they reach the value of *UpSafe* or *DnSafe*, they respectively increase or decrease their local value of maximum available colors and send a *kick* message. In a close vicinity where multiple readers are colliding, once they reach a threshold value they all send *kick* messages to reserve their colors hence the name Colorwave.

3) Probabilistic DCS (PDCS): PDCS [21] is another improved version of DCS and the first derivative to propose a multichannel solution. A parameter p is introduced as the probability for a reader to change its color after a collision. As such three cases are possible: case 1, readers involved in the collision do not change colors, they send *kick* messages that will induce neighboring readers to change color; case 2, one of the readers changes color and sends a *kick* message to reserve the color, the other reader interrogates tags with previous color without changing; case 3, both readers change colors, in this case both readers send *kick* messages and reserve their new colors, this is the casual algorithm of DCS. However, as with DCS, the maximum number of colors is fixed inducing the same issues, and a probabilistic-Colorwave was also proposed.

4) Distributed Color Non-cooperative Selection (DCNS): DCNS [22] is yet another derivative algorithm of Colorwave. The first difference with Colorwave is that readers here do not send *kick* messages updating their maximum color value, μ. Another introduced parameter is η which determines the probability for a reader to interrogate tags once at its timeslot. As such, readers are classified in 3 different types: *killer* for $\mu == 2$, with such a low color range, these readers get to frequently interrogate tags, therefore they do not send kicks nor change channel to avoid collisions with neighboring killers; *normal* for $2 < \mu < threshold$, these readers act as casual readers in Colorwave; *killed* for $\mu > threshold$, these readers constantly send kicks and rarely interrogate tags, they get to increase their value of η in order to increase their interrogation chances.

5) Distributed Efficient & Fair Anti-collision for RFID (DEFAR): In this protocol [23], authors propose a scheme to retrieve at least one of the contending readers in case of a collision. This improvement is made using beacon exchange between neighboring readers. Based on reader IDs and priority levels, a reader is chosen. The priority levels are set depending on the success of readers during previous contentions. Another version of this algorithm was proposed in [17] to address mobile deployments. While these solutions improve the fair access to shared medium among readers, they rely on a precedent beacon exchange which is itself subject to collisions.

6) Coverage Oriented Reader Anti-collision (CORA): CORA [17] is aimed at time critical RFID systems. After selecting a timeslot in the available range, readers exchange beacons to inform their neighbors. Each reader is then able to compute the number of colliding readers as well as the number of readers on different slots. Based on this information, readers then decide to read if they have more neighbors on different slots than colliding ones and get disabled if there are more colliding readers than non-colliding ones. This algorithm is based on the observations made in Section II-B where other readers, in case of a mobile deployment, can cover the previously missed tags due to collisions. To the expense of collisions, this algorithm improves the delay needed to cover tags in range hence the name.

7) MAximum LIkelihood COlorwave (MALICO): MALICO [24], brings yet another improvement to Colorwave relative to its convergence. Instead of relying on a set of thresholds and triggers manually inputted, readers automatically update their number of available colors to decrease collisions. The update is done by each reader following the observation of successful, colliding and idle slots in the previous round to estimate the number of neighbors. Based on this estimate, a number of available colors is set to maximize the throughput. This process has the advantage of dismissing the kick phases present in Colorwave to increase interrogations and throughput. However, MALICO needs to implement bi-static antennas on readers in order to listen and record possible collisions while they are accessing the medium. The protocol was tested both in static and dynamic scenarios and with reliable results. Nevertheless, due to the listening and computation for each reader, the performance is linked to velocity of readers in mobile deployments. Indeed, the computation can be done for a given state of neighbors during the interrogation round which unfortunately changes due to the mobility in the subsequent round. However, thanks to the simplicity of the process, computation cost can be kept rather low and not impact the interrogation rounds.

B. Centralized algorithms

In these proposals a central server is used to allocate timeslots to readers either randomly or depending on parameters like their positions, number of neighbors or performance on previous rounds.

1) Neighbor Friendly Reader Anti-collision (NFRA): In NFRA [25] interrogations are organized in rounds coordinated by a server. This coordinator at the beginning of each reading round sends an *Arrangement Command (AC)* advertising the maximum number of beaconing timeslots to chose from. At reception, each reader randomly selects a timeslot and waits for the corresponding *Ordering Command (OC)* from the server. They then send a beacon to alert neighboring readers of their intention to interrogate tags. If no collision is observed during the beaconing period, the reader then sends a *Overriding Frame (OF)* to disable all neighboring readers for the current round. Once a reader receives an *OF*, it awaits the next *AC* from the coordinator to compete again. In very dense deployments, this algorithm induces a high number of disabled readers due to *OF*s. Also, readers with a high timeslot value, have a greater chance to be disabled by their low timeslots counterparts.

2) NFRA+ & NFRA++: These proposals [26] are improved versions of NFRA as their name implies. The first NFRA+, corrects the above-mentioned drawback regarding high timeslot values. As such, this algorithm tries to improve the fairness by increasing the priority of readers that spend a long waiting time without interrogating tags. This priority increase reinforce the probability for the reader to chose a low timeslot value and vice-versa for low priority readers with a low waiting time. This affects the fairness of the algorithm but not the high number of disabled readers at each round. NFRA++ tries to correct this issue by providing a second chance at previously colliding readers. In this algorithm, after sending all corresponding *OC*s to the current round, the coordinator then sends yet another OC to readers that previously had colliding beacons. Readers determine a probability T to send a beacon in this ultimate OC. This gives a chance at colliding readers in current round to compete again with a probability T. Both the added layer of fairness and second chance combined allows this algorithm to have high performance.

3) Geometric Distribution Reader Anticollision (GDRA): As mentioned earlier, readers with a low timeslot value have a higher chance of interrogating tags and a lower chance of receiving an *OF*. This algorithm [27] corrects this drawback by using a geometric distribution called Sift [28] for readers to chose their random timeslots instead of the classical uniform distribution. Using this geometric distribution a few number of readers select a low timeslot value while all the others select a higher value. This allows to highly reduce the number of beaconing collisions that disabled readers for the current round. This algorithm shows really high performance but still suffer from the high number of disabled readers from *OF*s in dense deployments.

4) Fair Reader Collision Avoidance (FRCA): In [29], authors propose two versions of their algorithm. They both make observations regarding the lacuna in both NFRA and GDRA and address them. In FRCA1, readers follow the same scheme as in NFRA with a central server sending commands and readers randomly selecting slots and sending beacons. However, in case of a beacon collisions when two readers chose the same timeslot, instead of both getting disabled as in NFRA, they compare their number of successes. The reader with the lowest success rate gets access to the medium and the other one waits for the next round. This allows the protocol to be fairer regarding the shared medium access. In FRCA2, in addition to the success rate match, readers also compute the distance between them based on the received signal strength of the exchanged beacons. Based on the distance between them, the failing reader with the higher success rate, can compete on the next timeslot but on a different channel. Indeed, if the distance is greater than twice that of the reading range, the reader may interrogate tags next to its neighbor on a different channel. Authors also propose the use of Sift distribution in order to decrease the number of contending readers on lower timeslots.

5) Adaptive Color-based Reader Anticollision Scheduling (ACoRAS): In ACoRAS [14], instead of having readers blindly select a timeslot in an available range, the timeslots are assigned directly by the server following the construction of a *Minimum Independent Set*. Using knowledge about the deployment of the readers (colliding neighbors, position, covered tags, ...), the server affects a set of colors to each reader ensuring it will not collide with others in its vicinity. An optimization algorithm is then run by the server to reduce the number of distributed colors to lower the latency and idle time of the system. This is done by leveraging the tags that are covered by each reader. As such, if a tag is covered by multiple readers at the same time, the server only affects a color to one of the readers and disables the others for the current slot. While this algorithm can provide very low to no registered collisions and missed tags, it relies on a high overhead in order to determine the optimal color distribution and cannot be considered for an uncontrolled mobile deployment.

6) Geometric Distribution-based Multiple Readers Scheduling Optimization Algorithm using Artificial Immune System (GD-MRSOA-AIS): As the name implies, in [18], readers use a geometric distribution, Sift [28], in order to decrease the number of contending neighbors on lower timeslots. On top of that, an artificial immune system optimization is introduced in order to improve the scheduling scheme. The interrogation range is then more effective using the corresponding algorithm. However this algorithm relies on the knowledge of the readers deployment positions and fails to deal with mobile scenarios.

7) Centralized and Aligned Scheduler compatible with EPC-Global (CASE): In CASE [30], readers are allocated medium resources by a central server that has a global vision over the whole deployment. Apart from operating at different times, readers also operate on the different frequencies allowed by ETSI EN 302-208 [2] following the instructed configuration. Based on the position of readers, assumed to be known, the server allocates slots and frequencies to readers depending on their priority and distance from neighbors. This allocation is performed by solving a Mixed Integer Programming (MIP) problem which aims to: *(i)* maximize the total amount of slots allocated and *(ii)* ensure a fair distribution of the resource available. Using a weighing factor α to either maximize throughput and/or fairness and a set of constraints, the server is able to optimize the scheduling of readers' interrogations. The proposal was tested under a fair level of density and performances in terms of throughput quickly dropped with a growing number of readers. Computation cost is also a feature that has been looked upon and results show that it increases drastically with the number of readers deployed, the density of deployment, mobility or priority levels addressed.

V. CSMA PROPOSALS

A. Distributed algorithms

1) Listen Before Talk (LBT): This is the standard protocol for reader collisions [16]. In this proposal, readers "listen" to the medium during a defined period of time before attempting to "talk" (interrogate tags). If ever the medium is found occupied, the reader switches to a different channel and performs a new "listen" session. In case of a very dense environments, readers can be stuck in a "listen" loop trying to find an idle communication channel. Also this protocol would have very poor performance in a mobile scenario since a reader "listening" at a given place could not ensure an idle channel throughout its path.

2) Pulse: This protocol [15], just as LBT, has readers listening to the medium before interrogating tags. However, in this instance to prevent mobile listening issues, readers constantly "pulsate" a signal to alert their neighbors during operation. As such, when a reader receives the pulsating beacons, it disables itself and waits until the medium is clear. This had the advantage of making sure one and only one reader is interrogating tags in a given vicinity. Nevertheless, in a dense mobile environment, readers sending a "pulse" might end up disabling a lot of their neighbors highly impacting the throughput and efficiency of the system.

3) Anticollision Protocol for RFID: This protocol [31] uses beacons exchange between readers to estimate the distance between them and compromise over colliding covered tags. Indeed, after a backoff period, readers send a beacon. The backoff period is computed from the residual energy of each reader in order to avoid beacon collisions. The beacon informs neighbors about the covered tags and from the received signal power, readers estimate the distance between each other. After interrogating tags, readers then exchange information about the collected tags to neighbors. While this could help reduce collisions, estimating the distance between readers based on received signal strength is prone to errors. Also tags that are covered by a single reader colliding with its neighbors are disadvantaged.

4) High Adaptive MAC (HAMAC): In this algorithm [19], readers wait for a random backoff period within a defined Contention Window (CW). If the medium is busy, the reader switches to a different channel and checks if it is idle. If all channels are busy, the reader then divide the CW by 2 and draws a new backoff. The newer CW size allows the reader to have a shorter backoff period increasing its priority. The reader then performs the check on all channels once again. This process is kept until a minimum size of the CW. Once reached, the reader starts again with the highest CW size. While this solution tends to increase reading chance of readers, having different CW sizes among readers may increase latency for some of them then impacting the fairness for medium access.

5) Ditributed Multi-Channel Collision Avoidance (DiMCA): Slightly different from previously presented CSMA algorithms, the DiMCA [32] protocol proposes for readers to exchange messages on two different control channels operating at different ranges. The first one covering the reading range of the reader where messages containing the ID of the reader are sent and the second channel covers the interference range where messages containing both the reader's ID and its chosen channel are sent. Before interrogating tags, a reader waits for a random time period during which it can receive messages on the control channels. As such, depending on the type of message received, a reader keeps 2 queues of interfering neighbors: those for which he can operate at the same time but on a different frequency and those for which it has to operate different at a time. Before starting its interrogation operation, a reader checks its queue and depending on the state either chooses a different channel to operate on and broadcasts it to its neighbors beforehand, or waits for an END signal from its neighbors in order to operate at a different time. While this solution improves both the throughput and efficiency of the RFID system, it relies on an overhead created by the exchanged messages which can impact the delay. Authors also do not address how they avoid having collisions regarding exchanged messages.

6) Enhanced Distributed Multi-Channel (EDMC): EDMC [33] proposes an improved version of DiMCA by having readers check if they have received other messages from neighbors after they chose their channel and before sending their own message. This decreases the chance for message collisions or misheard messages from neighbors right before tag interrogation. Authors claim to slightly improve the delay as well as reduce the collisions using this technique compared to DiMCA.

7) Efficient Multichannel Reader Collision Avoidance (EMRCA): EMRCA [34] is an improvement of [15], to take into account multichannel aspect introduced by the standard. Authors identify two types of collisions based on the interrogation and interference range of readers. Readers start by sensing he common control channel used by all nodes to communicate. If no activity is detected during a given period, reader begins contending phase. Otherwise, depending on the source of activity, either starts a new listening session at the end of the current activity or, pursues the timer before contending. During contention, readers wait for a randomly drawn backoff. If a reader receives a beacon during this backoff, it goes back to sensing the control channel, otherwise if the backoff runs out without any reception of beacon, the reader moves on to tag interrogation. It then occupies the chosen interrogation channel and periodically sends out a beacon to advertise on the common control channel. This protocol improves the overall fairness and efficiency of Pulse but still suffers from mobility and high density of readers deployment.

B. Centralized algorithms

CSMA-based protocols rely on the readers listening to the medium as above-mentioned. As such, having a central server is superfluous since readers can be autonomous in such setups.

However, a few CSMA solutions are still centralized using a server to allocate resources to readers based on a global view and history of the RFID system. Its the case of HiQ algorithm. In HiQ [13], 3 entities are defined: readers, R-servers and a Q-server. The number and type of recorded collisions are communicated by the readers to the Q-server. Based on these information and using a Q-learning algorithm, the Q-server then defines the optimal slots and frequency distribution among the readers. A set of optimal slots are then given to R-servers to maximize reader operation. Readers are then granted slots by their responding R-server within their available set. However this algorithm merely describes the construction of this three-level topology. Also the complexity of the learning algorithm to find an optimal solution is correlated to the density of reader deployment. In case of a dense network, the complexity might induce an important overhead. Moreover, this algorithm would not be suitable in a mobile scenario with parameters permanently changing.

VI. Discussions

In order to evaluate RFID anti-collision protocols, multiple performance metrics are available and none of them, taken alone, can determine the best solution. In [35], authors review and analyze the state-of-the-art criteria for RFID anti-collision performance. As such depending on a given application and its needs, proposals can be tested and evaluated in order to determine the most performing solution. Among the proposed evaluation criteria, we retained the following ones:

A. Throughput

It can be computed using different metrics but mostly give the same outcome. Indeed, we can use the total number of Successful Query Sections (SQS) which can then be divided by the unit of time or/and by the number of readers deployed. A SQS is counted every time a reader successfully interrogates tags in its range. Another way of computing throughput is dividing the time spent by each reader when querying tags by the number of readers and total running time. This criterion assesses how often proposals schedule medium access to readers, however, it fails to indicate how well the medium is shared among readers (one reader getting the whole access throughout running time) or how this access is distributed in time (no reading for long periods of time due to overhead or complex algorithm).

B. Collisions

To the opposite of throughput described above, collisions are computed using the total number of Failed Query Sections (FQS). An FQS is counted every time a reader tried getting access to the medium to interrogate tags but was denied access either by the central server, in case of a centralized algorithm, or by its peers, in case of a distributed algorithm. But also, whenever multiple readers simultaneously got access to the medium in a given vicinity and tried interrogating tags in their mutual reading range, resulting in failed queries (see Section II-A). This metric assesses how permissive algorithms are regarding medium access to readers. An algorithm that records a high number of collisions is an algorithm that will unfortunately miss tags but also have a poor energy management.

C. Efficiency (Eff)

Based on the previous two given criteria we can compute the efficiency of a solution. This metric is computed as $Eff = SQS/AQS$ where AQS is the total number of Attempted Query Sections which is the sum of SQS and FQS. From this metric we can estimate how well a protocol can avoid collisions. However, this system efficiency can be misleading in case of a low throughput and low AQS as a whole. Indeed, an algorithm that granted 100 SQS and 11 FQS and another one with 10 SQS and 1 FQS end up with the same efficiency of 90% but it does not reflect how many tags could be interrogated.

D. Jain's Fairness Index (JFI)

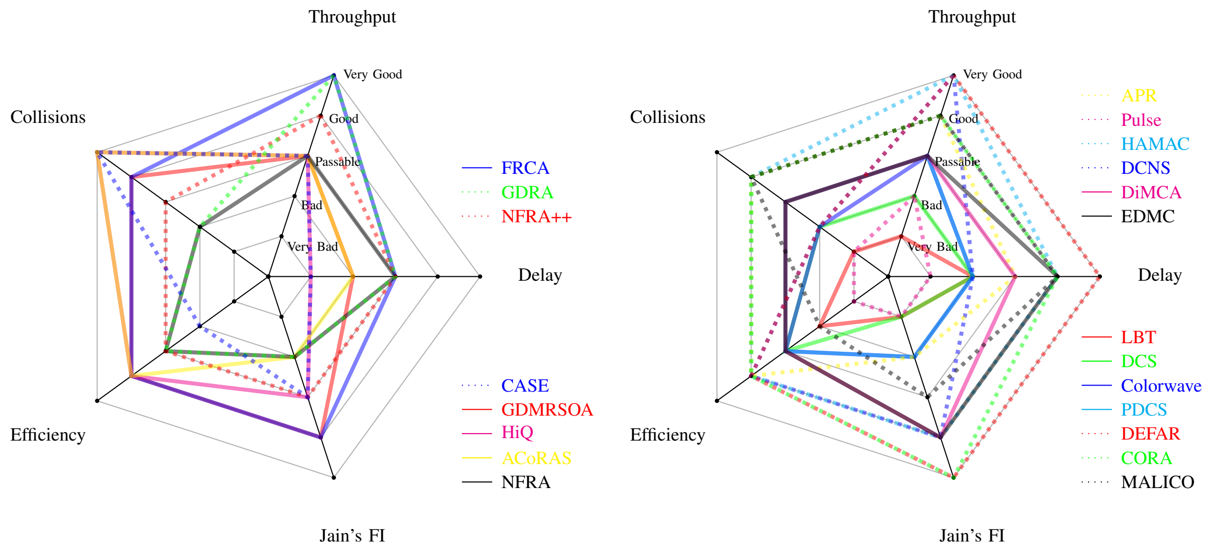
While the precedent criteria presented allow to know how an algorithm performs regarding collisions avoidance and efficiency, they however do not assess how well the medium is shared among readers. Indeed, an algorithm that consistently grants medium access to the same group of readers may have a high SQS but still does not means that all tags are being interrogated. All deployed readers need to have fair access to the medium in order for an algorithm to be fully efficient. The JFI is computed as follows: $JFI = \frac{|\sum_{i=1}^{n} x_i|^2}{n \times \sum_{i=1}^{n} x_i^2}$ where x_i is the SQS of the i^{th} reader. Using this metric, the performance of each reader has the same weight and the whole algorithm conduct both individually, at each reader, and globally is validated.

E. Coverage delay

Using this metric, we can know how long it takes to interrogate all tags in the deployment area. As explained in Sections VI-A and VI-C, a reader might have great results in those criteria but it does not reflect how well the medium is shared among readers and the algorithm might just be granting access to the same set of readers. Using the JFI, improves the judgment but in case of a algorithm that has a long convergence time, all the previous criteria might be high but it still does not make the algorithm reliable for some applications. Indeed, some scenarios may need the RFID system to quickly cover all tags deployed for tracking purposes and a high coverage delay can be a drawback.

F. Evaluation

Figures 3a & 3b, show an evaluation of the previously presented protocols over a Kiviat diagram regarding the performance criteria. Based on our observations, distributed TDMA-based algorithms are all-around less profitable than the others. This can be explained by their unawareness of the



(a) Centralized

(b) Distributed

Fig. 3: Evaluation

	Centralized	Distributed
TDMA	ACoRAS[14] FRCA[29] GD-MRSOA-AIS[18] GDRA[27] NFRA[25] NFRA++[26] CASE[30]	Colorwave[20] CORA[17] DCNS[22] DCS[20] DEFAR[23] PDCS[21] MALICO[24]
CSMA	HiQ[13]	APR[31] DiMCA[32] EDMC[33] HAMAC[19] LBT[16] Pulse[15] EMRCA[34]

TABLE II: Reader anticollision protocols

system configuration which can be very random in dense and mobile environments. Basing the readers activity on a local information at a given time is insufficient to have a proper working solution. DCNS offers high performance in terms of throughput and collisions as well as JFI but suffer from a needed convergence time to reach a stable performance capacity impacting the coverage delay. Centralized TDMA-based approaches offer a slightly better performance but suffer from the high number for disabled readers at each turn, which affects both the JFI and coverage delay. Indeed, the server handling medium access based on an optimized distribution does not necessarily take the tags distribution and the need for fairness into account. Regarding distributed CSMA proposals, LBT and Pulse have very poor performances compared to the others due to their high level of collisions which impacts the fairness and coverage delay. Also constantly pulsating beacons, in the case of Pulse, is a poor energy efficiency. However, HAMAC with its backoff management and multichannel access has a high throughput and better fairness but can suffer from high coverage delay due to multiple CW sizes and potential long waiting times before medium access. Centralized CSMA proposals, such as HiQ, could offer the highest throughput and lowest collisions levels but the time needed for their learning algorithms to converge make them profitable for time critical applications. Depending on the application requirements in terms of delay, energy efficiency or throughput, the choice of the protocol has to be different. An all-around solution for RFID systems is not really feasible at the current state-of-the-art. Even if centralized solutions may seem to be more productive, they cannot cover scenarios where readers are sparsely deployed over a large area.

Based on our observations, Figures 4 & 5 give insight regarding the ability of each protocol to perform under different constraints or requirements. Indeed, a protocol that performs well in terms of coverage delay and fairness interrogates tags faster since more readers are successfully enabled and read tags within range. Coverage delay and fairness give an upper hand in the case of dynamic scenarios with mobile readers and/or tags. Relatively, performances in terms of throughput, collisions and efficiency give an idea of the protocol in dense reader deployment environments. In such conditions, readers are not successful in their contention procedures and fail repeatedly while attempting to access the medium. Only a subset of readers is active and the corresponding tags laying

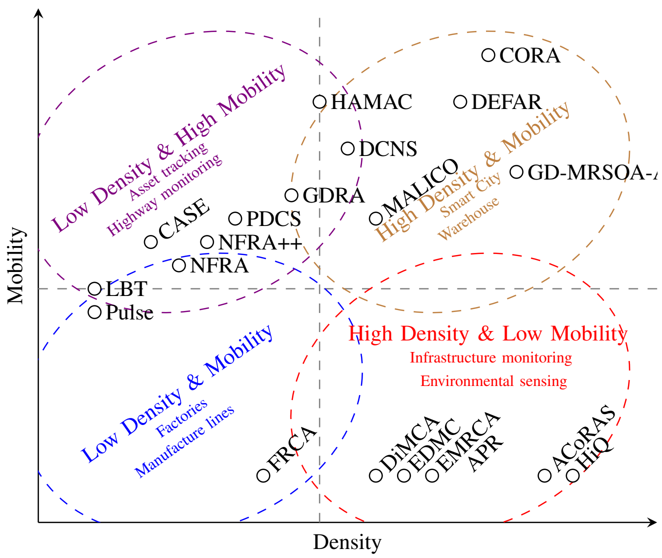
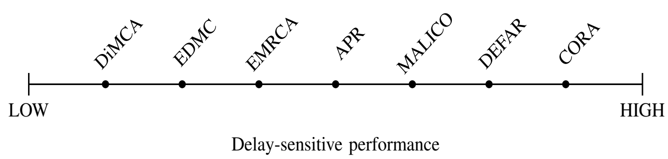
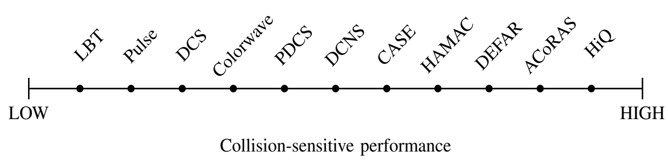


Fig. 4: Protocols performances in regard to potential applications requirements



(a) Delay-sensitive



(b) Collision-sensitive

Fig. 5: Protocols performances in regard to potential applications constraints

in range are interrogated. As such, the characteristics observed are:

- **density**: to know if the protocol can perform in very dense deployment scenarios where multiple readers are in close proximity. These scenarios can be found in factories where products have to be checked along the manufacture line;
- **mobility**: to check whether the protocol is able to handle mobile scenarios. This could be the case inside a warehouse with readers mounted on forklifts or in a smart city where readers are mounted on public transportation vehicles to sense parameters in the environment;
- **delay sensitive applications**: this validate whether the protocol should be considered when building a time sensitive application and tag information has to quickly be available. This could be the case in a sensing application where a critical issue might occur and all sensed data is vital;
- **collision sensitive applications**: these are applications where the least amount of collisions are expected in order to have a flawless working system. In the instance of a harbor where RFID tagged containers are loaded or unloaded from boats, collisions and missed tags could result in lost containers or thousands of goods.

For example, in order to monitor multiple boxes in a warehouse with fixed RFID readers attached to walls, where products have to quickly be identified and processed to avoid losses, a good solution could be to used DiMCA, EDMC or APR which can perform in dense deployments and delay sensitive applications. If ever, some readers have to be mobile (mounted on forklifts or hand-held by workers, a better solution would be to use either CORA or DEFAR which show high performance in mobile deployments. In case of a harbor, as mentioned above, with readers embedded on the ground and tags attached to containers, a solution like ACoRAS could offer the best trade-off; however, if some readers are mobile as well, using solutions like PDCS, DCNS or HAMAC is more reliable. In the instance of an RFID sensing application for agriculture, where readers do not necessitate a dense deployment in close proximity to monitor humidity and temperature levels, without critical data needing constant surveillance, Colorwave or LBT could be sufficient. If ever, one has to deal with readers attached to farmers or their mobile combine harvester, a solution like Pulse could be implemented.

Energy efficiency of these protocols should also be studied. In [36], authors evaluate the energy consumption of several RFID anti-collision protocols. Chosen protocols are both TDMA & CSMA, centralized & distributed to cover a wide range of proposals. Their results confirm the better energy efficiency of distributed approaches compared to centralized ones. Indeed, the cost of communicating with a central server in order to schedule interrogation activity is high due to the number of beacon exchanges needed. Our current work combined with results obtained in [36] should further guide the choice of a proper anti-collision scheme according to the application and deployment area.

VII. Conclusion

This paper presents a brief state-of-the-art review of the current RFID anticollision most known proposals. Issues regarding the deployment of RFID solutions are presented and explained to understand the challenges needed to be overcome. It describes the operating scheme and states the strengths and weaknesses of the different proposals dispatching them in either TDMA or CSMA, centralized or distributed algorithms. Most relevant RFID performance criteria are also introduced to better assess the proposals operation. Protocols are then compared based on these criteria to identify how they perform on different metrics. A short discussion then argues that the choice of a solution or another should be application driven in order to cover its needs and requirements. Multiple research directions can be derived from this work regarding the use of RFID for different applications such as sensing for smart environments, data collection of tag information, RFID security or improved energy management.

ACKNOWLEDGMENT

This work was partially supported by a grant from CPER/FEDER DATA, the National Research Foundation (NRF), the French ministeries of education, research and innovation (MESRI) and Europe and Foreign affairs (MEAE), the LIRIMA Agrinet project and IPL CityLab@Inria.

REFERENCES

[1] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification.* John Wiley & Sons, 2003, ch. 3, pp. 29–61.

[2] ETSI, "Radio frequency identification equipment operating in the band 865 mhz to 868 mhz with power levels up to 2 w and in the band 915 mhz to 921 mhz with power levels up to 4 w; harmonised standard covering the essential requirements of article 3.2 of the directive 2014/53/eu," 2016.

[3] S. Kim, R. Vyas, J. Bito, K. Niotaki, A. Collado, A. Georgiadis, and M. M. Tentzeris, "Ambient rf energy-harvesting technologies for self-sustainable standalone wireless sensor platforms," *Proceedings of the IEEE*, vol. 102, 2014.

[4] R. Want, "Enabling ubiquitous sensing with rfid," *Computer*, vol. 37, 2004.

[5] I. Zalbide, E. D'Entremont, A. Jiménez, H. Solar, A. Beriain, and R. Berenguer, "Battery-free wireless sensors for industrial applications based on uhf rfid technology," in *SENSORS, 2014 IEEE*. IEEE, 2014.

[6] M. Bartholmai, S. Johann, M. Kammermeier, M. Müller, and C. Strangfeld, "Transmission characteristics of rfid sensor systems embedded in concrete," in *SENSORS, 2016 IEEE*. IEEE, 2016.

[7] M. Cassel, T. Dépret, and H. Piégay, "Assessment of a new solution for tracking pebbles in rivers based on active rfid," *Earth Surface Processes and Landforms*, 2017.

[8] R. V. Aroca, A. C. Hernandes, D. V. Magalhães, M. Becker, C. M. Vaz, and A. G. Calbo, "Application of standard epc/gen2 uhf rfid tags as soil moisture sensors," in *Multidisciplinary Digital Publishing Institute Proceedings*, vol. 1, 2016.

[9] R. Ramirez, E. Rojas-Nastrucci, and T. Weller, "Uhf rfid tags for on/off-metal applications fabricated using additive manufacturing," *IEEE Antennas and Wireless Propagation Letters*, 2017.

[10] K. K. Dheeraj, C. Kwan-Wu, and R. Raad, "A survey and tutorial of rfid anti-collision protocols," *IEEE Communications Survey & Tutorial*, vol. 12, no. 3, 2010.

[11] D.-H. Shih, P.-L. Sun, D. C. Yen, and S.-M. Huang, "Taxonomy and survey of rfid anti-collision protocols," *Computer communications*, vol. 29, no. 11, 2006.

[12] M. Bueno-Delgado, J. Vales-Alonso, C. Angerer, and M. Rupp, "A comparative study of rfid schedulers in dense reader environments," in *Proc of Int. Conf. on Industrial Technology (ICIT)*. IEEE, 2010.

[13] S. S. J. Ho, D.W. Engels, "Hiq: a hierarchical q-learning algorithm to solve the reader collision problem," in *Proc. of Int. Symposium on Applications and the Internet Workshops, SAINT*, USA, 2006.

[14] E. Hamouda, N. Mitton, and D. Simplot-Ryl, "Reader anti-collision in dense rfid networks with mobile tags," in *Proc. of Int. Conf. on RFID-Technologies and App. RFID-TA*, 2011.

[15] S. Birari and S. Iyer, "Pulse : A mac protocol for rfid networks," in *Proc. of Int. workshop on RFID and Ubiquitous Sensor Networks (USN)*, 2005.

[16] "EPC TM radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz - 960 MHz version 1.2.0," EPCglobal Standard specification, 2007.

[17] A. A. Mbacke, N. Mitton, and H. Rivano, "Rfid anticollision in dense mobile environments," in *Proc. of IEEE WCNC*, 2017.

[18] L. Duan, Z. J. Wang, and F. Duan, "Geometric distribution-based readers scheduling optimization algorithm using artificial immune system," *Sensors*, vol. 16, no. 11, 2016.

[19] I. Amadou and N. Mitton, "HAMAC: High adaptive MAC protocol for dense RFID reader-to-reader networks," in *Proc. of AdHocNets*, 2015.

[20] J. Waldrop, D. W. Engels, and S. E. Sarma, "Colorwave: an anticollision algorithm for the reader collision problem," in *Proc. of ICC*, 2003.

[21] F. Gandino, R. Ferrero, B. Montrucchio, and M. Rebaudengo, "Probabilistic dcs: An rfid reader-to-reader anti-collision protocol," *Journal of Network and Computer Applications*, vol. 34, no. 3, 2011.

[22] ——, "Dcns: An adaptable high throughput rfid reader-to-reader anticollision protocol," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 5, 2013.

[23] A. A. Mbacke, N. Mitton, and H. Rivano, "Distributed efficient & fair anticollision for rfid protocol," in *Proc. of WiMob*, 2016.

[24] M. V. Bueno-Delgado and P. Pavón-Mariño, "A maximum likelihood-based distributed protocol for passive rfid dense reader environments," *The Journal of Supercomputing*, vol. 64, 2013.

[25] J.-B. Eom, S.-B. Yim, and T.-J. Lee, "An efficient reader anticollision algorithm in dense rfid networks with mobile rfid readers," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 7, 2009.

[26] R. Ferrero, F. Gandino, B. Montrucchio, and M. Rebaudengo, "A fair and high throughput reader-to-reader anticollision protocol in dense rfid networks," *IEEE Transactions on Industrial Informatics*, vol. 8, no. 3, 2012.

[27] V. Bueno-Delgado, R. Ferrero, F. Gandino, P. Pavon-Marino, and M. Rebaudengo, "A geometric distribution reader anti-collision protocol for RFID dense reader environments," *IEEE T-ASE*, 2013.

[28] K. Jamieson, H. Balakrishnan, and Y. Tay, "Sift: A mac protocol for event-driven wireless sensor networks," in *Wireless Sensor Networks*. Springer, 2006.

[29] H. Rezaie and M. Golsorkhtabaramiri, "A fair reader collision avoidance protocol for rfid dense reader environments," *Wireless Networks*, 2017.

[30] M. V. Bueno-Delgado and P. Pavon-Marino, "A centralized and aligned scheduler for passive rfid dense reader environments working under epcglobal standard," *Simulation Modelling Practice and Theory*, vol. 34, 2013.

[31] H. Rezaie and M. Golsorkhtabaramiri, "A fair reader collision avoidance protocol for rfid dense reader environments," *Wireless Networks*, 2017.

[32] H. Safa, W. El-Hajj, and C. Meguerditchian, "A distributed multichannel reader anticollision algorithm for rfid environments," *Journal of Computer Communications*, vol. 64, 2015.

[33] Z. YuJing and C. Yinghua, "Edmc: An enhanced distributed multichannel anti-collision algorithm for rfid reader system," in *Proc. of American Institute of Physics Conf.*, 2017.

[34] Y. Jiang, R. Zhang, W. Cheng, and W. Sun, "An efficient multi-channel reader collision avoidance protocol in rfid systems," in *Proc. of Wireless Communications and Networking Conference (WCNC)*. IEEE, 2016.

[35] F. Gandino, R. Ferrero, B. Montrucchio, and M. Rebaudengo, "Evaluation criteria for reader-to-reader anti-collision protocols," Politecnico di Torino, Tech. Rep., 2012.

[36] M. Golsorkhtabaramiri, N. Issazadehkojidi, N. Pouresfehani, M. Mohammadialamoti, and S. M. Hosseinzadehsadati, "Comparison of energy consumption for reader anti-collision protocols in dense rfid networks," *Wireless Networks*, 2018.